DECEMBER 6, 2018 EXPERTS' CONFERENCE

Legend:
AA – Alexis Arena
AW – Adam Wolek
JB – Jennifer Bayuk
KT – Kevin Tuten
BW – Bill Wagner

[Welcome to the Taft Stettinius & Hollister conference center. Please enter your passcode. Please hold while I confirm your passcode. Thank you. Your passcode is confirmed. Please wait for the tone, then say your name and press the pound or hash key.]

BW: Bill Wagner

CC: When you hear the tone you will be the third person to join the meeting.

BW: Hello, this is Bill Wagner.

AW: Hey, Bill. Adam's on the line. I believe Kevin Tuten is on the line as well.

BW: Good morning Kevin. Good morning Adam.

AW: Good morning Bill.

BW: So, we spoke with Alexis the other day and decided we should record our conversations. So, Kevin, this call's being recorded just to give you a heads up.

KT: Thank you.

JB: Good morning. Jennifer is on.

BW: Good morning Jennifer. You have Kevin Tuten, Bill Wagner, and Adam Wolek.

AW: Good morning Jennifer.

JB: Good morning Kevin and um Adam.

KT: Morning Jennifer.

BW: And, uh, this call is being recorded just so you know.

JB: Okay.

AA: Hello.

BW: Yes, we're uh. Is that Alexis?

AA: Yes.

BW: Hey Alexis, it's uh – I'm recording this call. This is Bill Wagner. I have Kevin Tuten, Adam Wolek, Jennifer Bayuk and me on the call.

AA: Okay, sounds good.

JB: Kevin, are you comfortable with the call being recorded because it doesn't have to be. There's no requirement that it be recorded. So if, if you're not

KT: I'm, I'm fine with it being recorded at this time.

BW: Well, I think the purpose of the call is just to, um, establish the protocol that's going to be eventually signed off by the parties, so um – I know Jennifer has some questions, if you want to begin.

JB: Sure. Um, I, uh, the questions all have to do with what the evidence is that we are being asked to search, what format it's in, what programs um we would use to search it, and um, if you remember from our last call, I'm sure you do Kevin, what – how we'll establish those um parameters of the data itself. Like, the count – the total count of records and the logs that we will search, what will be the search output – like the full log, and if we could see an example of an output that looks like a user just harmlessly browsing, examples of output that look like a user logging in, and an example of output that is obviously looking malicious. So if we can start out with, you know, knowing what the data looks like, what a search result will, uh, query result will look like, then as we uh use the IP addresses from RWF we can align them with one of those categories, and overall know that the number or percentage-wise, um of traffic that the um RWF IP addresses respond to versus the entire population. So . . .

KT: Well, quickly, Jennifer, um I was asked before to only do a search with an IP not worry about uh good traffic, bad traffic, or anything of that nature just to see if the data shows anything from the IP scope, then we can actually start drilling down to more in depth items. Um, it was more or less a simple search. My understanding is that – I have not looked at the data yet. Um, the data is a binary format. Um, there is a search tool that they have, um, that we will basically be using. My understanding is it's a virtual machine that has a copy of the data. Uh, we will log in through a zoom or a share of some type and watch each other search.

JB: Right. Well, if that were the case, then how would we know what the data is that we were searching. How would we answer the questions when we got a result whether or not it was malicious?

KT: I, I don't know that we're looking to try to do malicious at this point. They just want to see if their data, even in, in the list, it may exonerate, it may not. They just want to see if any of the data set matches.

JB: Okay. How do you know, Kevin, that if you are in a virtual machine using an unknown tool and have no direct access to look at the data or even try to translate it from binary or back or have a method of doing that, how do you know you're doing anything other than, you know, a PowerPoint?

KT: Other than .. .

JB: You want to be by – by

KT: I, I understand what you mean. Um, I also have asked for a copy of a record type, um, just so that I know the fields that I have to use. Um, but I have not gotten with them over that yet um because we were still so up in the air over the IP per se, um but I have not tried to go forward with that at this point.

JB: So you would agree that if we're searching a record we should have a copy of the fields in the records that we're

KT: A copy of the fields, yes.

JB: And, um, coming back to my original question, um, if you don't know the data format and you don't know how the tool works, how can you provide assurance that you have actually even searched anything other than you know how to pop up results through a piece of software that could be anything.

KT: Without doing some looks at the system when we get a, a chance to look, I, I can't say positive or negative one way or the other. I was going to do that if we got access to the system. Now, being the data sets are as large as they are, um, the search tool that they're using is, from my understanding, a, a standard, a standard tool for binary searches. Um, I can't remember what the name of it was off the top of my head. Um, but it, it's freeware.

JB: Oh really? Um, well, then if we had access to the data we should be able to do things like find a, a customer who would normally be in that data. You know, put their IP address in and have that customer's record, um, in the form of a log come back. And then we would see the log and then we would know the field. So maybe if we had access we could start by examining the program, examining logs that we know are there, and maybe doing some kind of baseline to find out how many records are in the actual data source so that we can get to the data source and we know what one record looks like, we can see the size of the data source and divide. Well, somehow get to an estimation. Would that make sense?

KT: It makes sense. Like I say, I, I have yet to put my hands on the data source. I have, I have seen sort of the record types. There's a lot of, lot of fields per record, if they're storing everything that I think they are. I just don't know how much I just don't know how much they want to display their record types and their record layouts for their, the way they use it for their software.

AA: If you have a specific request for viewing something, other than what we propose to do, I'm going to have to take that back to them for approval.

JB: Yea, I don't think, um, I think my requests are pretty consistent, what, what the traffic, what bad traffic looks, the number of records, and what um the search program

KT: I didn't know that we were – from what I was requested, they, they weren't looking for good traffic, bad traffic – they were just looking to compare the IP addresses against the data set. That's all – whether you get a positive find or not.

JB: Alright. In our last conference, um, we discussed this and my question to you was how would you decide whether the traffic was malicious or not if you didn't have some example. All you would say is because the IP address is in there it must be bad. And as you can imagine, that's not actually a, a leak.

KT: I concur with our earlier discussion. However, I think what they're want to do is go is there something to even concur about. Let's see if there is data that shows up. If so, let's spend some more time and go through round two of what is good, what is bad, uh, of that nature. Um, first pass is – is there anything here?

JB: Uh huh. So, if we were to do that then we would have to know that the second time we were searching the same data sets as we were searching the first time, in which case we would have to have some way of um fingerprinting the data sets.

KT: It's my understanding the current data set is read-only, uh copies, that can't be modified or changed. Uh, they are you know points in time and multiple copies of them. So, I, I don't see how we could modify the data set or the data set can be modified if it was written with a timestamp already.

JB: Um. Yes, it would be great to have that protocol and to understand that and to be able to verify that. So, I mean, if there is a, a chain of custody with a copy procedure and a timestamp and we could examine that, then I would have the same assurance that that you are talking about, but I don't have that now.

KT: I, I have not looked at it but that was what was uh my understanding. Uh, Alexa can probably get that from Patrick. Um, with how, how that whole chain of custody works currently with their system.

JB: That sounds great. Alexa do you think you can get that chain of custody from Patrick?

AA: To be clear, all you're asking for is

KT: The process

AA: When was this preserved, when was the mirror created per the judge's instructions. Yes, I mean obviously we're going to need to, to do that because those are all fair, fair questions. You

know when, when we get to witness testimony, I would assume that RWS's attorney would be asking all of those, those questions before any evidence is submitted into evidence so that – do you understand that?

JB: I am. I agree that it will come up then, but it is also part of the protocol for examining the evidence to actually have that baseline of what it is we're examining.

AA: Okay. Yes I can go back to HomeSource and I mean, I instructed them everything should be preserved, timestamped, mirrors should be created, you should not be having access to the mirror that the, um, experts are searching. I think that is consistent with the judge's instructions, so that is what everyone is trying to do.

KT: I would just ask HomeSource to uh display the, the procedural process on how that, that occurs to show them it is mirror copied and you know, what's mirror copied it, it's never touched again.

AA: Okay.

JB: And then the method, what we would be doing is we would devise a method to verify whatever that was. So once we saw it we could say oh look, they preserved it by uh copying it to disc and this particular program creates a cryptographic hash ___ at the end of the copy to demonstrate that the read-only has not been tampered with, so if we run the same algorithm on that same data, we should come up with that same string which is really what I was calling the fingerprint, footprint for it.

KT: Fingerprint, yep.

JB: Fingerprint. Right. So, so then the protocol would be we have that info, we reproduce the fingerprints so that we're starting on the same page, we examine the data translation program if it's open source, we could even download it ourselves and you know do the same query.

AA: Uh hum.

JB: The, uh, so then the only thing we really haven't addressed is context. Um, if there is an IP address in the record, that record is something that we had called the output of the search, not simply a true or false that the IP address was there, but what type of record it was part of. So, I have proposed a set of labels for the record called um, you know, "Log In, Browse, Malicious". Um, if you have a different set of categories for the record, I think Kevin you said that there were multiple categories for the records maybe, we could share that list and then we got a record back, we would know it was one of those.

KT: Once we can see the record type site, I, I don't disagree.

JB: Mmm hmm.

KT: Um, I'd imagine, like I say, usually, usually I go through the process of how far, how far in do I need to go? Um, am I going to spend all of my time defining good and bad initially to search and not know, whereas I can search with my parameters that I am starting with that I might have something and then I have to go in to good or bad.

JB: Um. That.

KT: I like to narrow it down that way first. So that

JB: If it's an internal investigation, that's fine but if we have to agree on a protocol where the uh the parties that have the IP address is automatically going to be assumed that, then we really want to know what that record looks like first. For example, let's say that that record contains um, uh, frames of other uh photos from other websites, which these retail websites often do. Right? So there's a product and the manufacturer has a, um, uh, manual for that product. Say you're browsing it, you want to look at the manual. When you click on that link from that website you're actually pulling that manual from the manufacturer's site. Let's say the web server pulls it from the site for you on your behalf to serve it up to you. It's very possible that manufacturer's website would be in some record in the application log. So, the fact that there is an IP in application logs because they can be so incredibly diverse does not mean that that IP was anywhere near the application. It just means that it was a data point at some point being used by the application. So, at least we need that difference.

KT: I don't disagree with that particular statement at all.

JB: Uh huh. Okay. So, so we actually do need something that we call a, a user activity log, you know, that that would actually be indicative of uh a external website, external IP visiting the application, as opposed to any other record. And then within that user activity there are going to be completely harmless things like browsing, and then there'll be something malicious which has yet to be named, but there would be a category of record, presumably, which may or may not include malicious stuff, and then there would be a record of a log in which would then link the IP to an identity. So any record that links the IP to an identity would obviously be a record of a different, different type than a record that was browsing. So, if we could have examples of these records, know how many of each are in the data sets, then we would have some context with which to interpret the results. And that's all we're looking for here – context for the result. It might not be a priority for HomeSource to have this context because they have the context already. They know it without having to have it defined, but seriously, neither one of us will know what this data means unless we have it.

AA: So here, here's – I think we're getting ahead of ourselves a little bit. Like with the, the cyber attack analysis. We're going to do this very simple search, there's going to be an output. That output will be designated attorneys' eyes only and shared with both experts and both counsel. At that point, we can then look at the, the output and RWS can make arguments as to what it means, and how to interpret it, and how to label it. Right?

JB: I think you're going off in a, in a direction that we are not technically prepared to do. We can't make any assumptions about what anything means without having, in advance, some

direction from HomeSource on how to interpret this data. We won't know. And as far as us going ahead of the cyber attack analysis, this is step 1 of a cyber attack analysis. This is an integral part and a foundational part of the cyber attack analysis. We cannot go into this step thinking that this is not a cyber attack analysis. Otherwise, why even bother?

AA: I'm not sure, I'm not sure we're understanding each other. So, my point is we're going to get these results. The results may say no IP shows up anywhere in the log. If that's the case, then there's nothing to analyze, and there's nothing else to do.

JB: Then it's over. Then, this cyber attack analysis will close. But it will have started as a cyber attack analysis.

AA: Okay. Again, I don't think we're – I mean, it's not, not necessary

JB: Okay, first of all, just to correct the record since this is recorded

AA: The cyber attack analysis may not be over if we can get a complete list of IPs. Okay, so this assumes that we have all of the IPs utilized by our, all RWS employees and principals and agents.

AA: Assuming that we have a complete list of IPs, which is a big assumption, and nothing comes out, there's no evidence to, to analyze, then I, then I would expect that nothing happened, that was caused by RWS. Um, so that's step 1 for us. You know, did something happen? If we do have results come out, then I would expect there would be a second step where we do discuss what those mean, and figure out what those mean through discovery.

AW: Alexis, as a reminder, this is an expert's conference, the judge has directed both HomeSource's and RWS's expert to come up with the protocol. Again, that's supposed to be the attorney, it's not supposed to be you, it's not supposed to be I who makes these protocols. It's the experts. But, uh,

AA: Adam, I would like to ____ a protocol right there.

AW: We, we should turn it back to the experts – it's an experts conference.

AA: Okay. Your point has been made. Um, if I could just finish. I was discussing something with her and I don't think we were understanding each other. So that's why I'm, I'm interjecting there.

AW: It's really for the experts to understand each other. It's an experts' conference for them to establish a protocol. The judge was very clear about it.

AA: Your point has been made. Your point has been made. The parties have . . . Adam . . .

AW: Alexis, please don't interrupt me.

AA: You're interrupting me. You're interrupting me.

AW: I was speaking. Um, please let the experts continue. It's an experts' conference and uh, you know you're interjecting and arguing with the expert. Uh, I don't think it's for the _____ expert's progression and establishment of a protocol. So I suggest you

AA: Adam, are you done?

AW: The court directed – I'm still speaking – uh, I suggest like the court directed, to have the experts talk and come up with a protocol. It's not up to the lawyers, it's up to the experts.

AA: Okay. You've, you've repeated that point and made that point. My point is the parties are represented by counsel on this call, the parties have to sign off on the protocol, the parties have to understand what the protocol is to sign off on it, and that is why I'm allowed to speak. And I would appreciate it if you would stop trying to silence me. I'm doing my job.

AW: No, no you're actually not. Um, the court has stated that the experts are supposed to establish a protocol. They have yet to establish a protocol. Let them speak, establish a protocol, and then like your client, our client will also review that protocol. Um, but until that time we shouldn't be interrupting the experts. Again, it's an experts' conference.

AA: I wasn't interrupting her. I'm having a conversation with her and you're trying to prevent me from doing that.

AW: No, it's an experts' conference, it's for the experts it's not for us.

AA: Okay. Your, your point's been made. I think we can move on.

JB: Okay. So, let's go back to uh, step 1 of this uh – I think so far, Kevin, let's, we've agreed on some things, so I'd like to go ahead and uh lay that out as part of our protocol that we have the uh, the chain of custody as we are calling it, that we have a method to verify that, that um,

KT: Verify chain of custody process.

JB: Uh huh. Uh, that we have some, and this is where I was getting, that we need to know what record types are in there and how many. Can we just agree on how many first? I think that should be easy. How many records are we searching? Being searched?

KT: Um. I, I have – I do not know how many records. I know there's lots of records.

JB: So we need a method to estimate how we fig

KT: Um, I'd imagine the first will be, uh, what is the timeframe of the record search? Is it from the dawn of time to a current point in time? Or is it a specific set of months?

JB: Uh huh. Yep.

KT: That will win at the record set.

JB: That's good. And then, maybe there – because we will have a way to query the data, at that point we can just query the timeframe and get the, the total record.

KT: Agreed.

JB: Now we're at the point where um we're trying to establish that there are different record types in the record sets, and because this is Step 1 in a cyber security investigation, as we agreed last time and you just agreed again, although you mentioned that it wasn't your direction to do anything other than find the IP address. In order to make a conclusion about whether the, um, data in the record is deemed malicious or not, uh knowing the record type is an essential, um, component of an analysis from whether or not, um, activity is malicious.

KT: For maliciousness, yes. Knowing record types, we'll help define and um apply for those particular types of, good or bad. I, I do not disagree.

JB: Alright. So if there is an IP in the record, and Step 2 is to determine whether that activity is malicious, then getting that activity record in Step 1 as a result of the search is actually making the search more efficient. Otherwise, once you have a set of IPs you gotta go search again and get the record types.

AA: We can do another search later, if needed.

JB: I know, but that leaves us without a result of the search, and it's my understanding we are entitled to a search result.

AA: No, there's going to be a search result. You will get a search result. There will be a search result. The result will say if RWS's IPs are in the logs and if they are, there will be an output showing what information they're associated with and the logs. That's my understanding. Kevin, please correct me if that's wrong.

JB: In order for both of us to complete our analysis, we will need ongoing access to that data screen to redo the search ourselves independently.

AA: We're not going to give experts ongoing access to

JB: Then we both have

AA: [*talking over JB*]

JB: Then we won't have any results. We are entitled to the same set of results.

AA: Maybe I'm just not understanding what you're saying, but my understanding is we're going to do a very simple search to see where RWS's IPs appear in the log. We will get output

from that search. It will show if they appear or not and if they it will show data associated with that appearance. That data will be printed out and designated attorneys' eyes only. You can keep that data. You can take it home. But you will not have ongoing access to the database. After the search is done and that output has been created, the database will no longer be available.

JB: Now we're getting somewhere. Um, so Kevin, uh let's go back to agreeing on the context. Alexis has just said that we will get data back. Can we define what that data is in a way that we will know whether or not we have that data?

KT: Um, that will be in the fields displayed, from my understanding, yes.

JB: Okay. So then we need to know what fields will be displayed, post search. Like, what, what's the result of the search. Like – and agree that there are enough fields to understand what that record is. And that's why it would just be so much easier to have a list of the record types in the field. Otherwise we're making it up.

KT: Gotta have, we've got to have the actual record type, a record designation with the field, per record. How many fields are in a record?

JB: Uh huh.

KT: Is it 5,000, is it 5?

JB: Right. And if it's 5,000 some way to get to the most germane fields to have a unique identifier.

KT: Correct.

JB: Okay, so if we have those defined in advance then we'll know what the output is when we see it.

JB: So, we've agreed now on the method to verify, a method to um query. Now, the unclear part for me right now is this search tool and how we can verify that if we run this program against this data it will actually produce something that's coming directly from that data as opposed to, you know, going off to some other data source in the internet to find something. So, um, knowing how that program works, uh what the actual connection point between that program and our mirrored data set is, and being able to test that, maybe by like writing a stub and seeing that we get the same test result from our stub as we do from the program, this might be uh an easy way to go. But without actually, you know, having that program defined and um, it's – when we get to whatever source that we're, you know, that whatever conference that Zoom, whatever, that we're looking at, we will not have, um, any assurance that the program is operating as expected. So, I'll just throw it out to you, Kevin. What do you think would be a good way to get, um, assurance that the program is, you know, not just vaporware _____.

KT: I've been thinking about that a little bit. Um, being able to verify the config string for the database or the data location, um, points to the read-only logs. Um, verify that there has been no modification to the host records or uh, host logs to redirect for DNS, um so that nothing's being redirected, excuse me just a moment.

JB: Okay.

KT: Sorry about that. Do, do a, a system inspection is the only thing I can think of initially. Um, being able to validate where they say the current logs live, if we have a method to do that, then test it from the system that we're supposed to use, make sure that they comply or equaled so that I know I'm getting real data and not a, a spoof data set.

JB: Uh huh. When you say current logs, do you mean like um like go into the current site knowing what your IP address is and then using the program to look at the current logs to make sure you come up with your own activity or?

KT: Um, I don't know if it's home activity. Uh, my understanding is the logs will only have, be available to this particular box, uh the mirror copies, so they won't have access to the live logs.

JB: Okay. Okay. So when you say current, you just the, the ones that came through the chain of custody, then.

KT: Correct.

JB: Okay. So when we're talking about, um, verifying that we're touching that data, uh there is still, as, as you know from um Reflections on Trusting Trust? To – I don't know if that paper is still in your mind, but it was a big, uh, ____ in computer security and it was the one where um, um, Ken Thompson won the Touring Award for saying that no matter what program you run, you will never know whether it's really running what you think it because the compiler always could have introduced something different, ____ if you're reading the source code you don't really know that's what you're running. So, um, that's the, uh, I'm not going to go to the - into the compiler level, but, um, if there is a programming language that that search is written in, it's appropriate to look at it and make sure that, if you agree, that uh, if, you know, given the data set that we have defined, if you type in the IP address that you know, matching record will come out.

KT: Verification of the search tool.

JB: Right. Now if we were given the search tool in advance, we could verify it then, but otherwise we would need to see the codes underlying it at some point and know we were running that code.

KT: That, uh, that I would have to ask HomeSource on what their search, the search tool is in advance and if it can be shared.

JB: Right. If it's open source, then I, I think that would probably lean in the direction of why not. Um, would you agree?

KT: As long as – yes as long as it hasn't been modified for their, their internal use – I have to ask.

JB: Uh huh. Well, even if they said it's based on the open source program X, then we spring the open source program X, modify however we wanted to based on what we were told the query data is, we'll have the string, right, that connects us to the database, and we should get something. Right? And that would be enough of a verification for me.

KT: I don't disagree.

JB: Okay. So, I think we've agreed all ____, except for actually, you know, knowing whether something's malicious or not, I think I'm gonna leave those things to the – as long as we have the list of the types of records that we have and the data fields that they're in, um, then we can, um, leave the determination of malice uh, to Step 2. Right?

KT: Yea.

JB: Okay. So, um, I, I can recap or, or if you want to I, I think we've gotten far enough to say, you know, you, you may do a little digging with yoru client to get the actual data behind our generalizations here and then you could do a first draft of the protocol because you would actually have that info and if I did the first draft, it would just be blank. Right? I mean, have a lot of blanks in it.

KT: Right.

JB: Right? And

KT: And then share it with Alexa and she could share it.

JB: Right. Right. And, uh, if I have comments on it or ___ have a nuance or a uh word in my notes that didn't correspond to it, we could do a duration or two but I'm sure that we'll just hone it down until we can agree on the search.

KT: Okay. So, initial is to write out our protocols, uh, exchange so that we are on the same page

JB: Uh huh.

KT: Through Alexa or through the attorneys, um verify that we are together and then set up a time to begin the initial search.

JB: Sounds good. So, do you want me to recap the, uh, the protocol notes that I have or you, you can probably just listen to this recording later and get it as well. So up to you.

KT: Um, the ones I have are where we verify the uh process for the chain of custody

JB: Uh huh.

KT: Um, verify the point of time that we're searching, come up with the total number of records based on point of time, um record type inside of all the fields displayed for a, a single record to help with phase 2 if needed.

JB: Right.

KT: #3 – unique identifier to validate the uh data is valid, and 4 to verify that the search tool is valid.

JB: Good.

AA: Does that all sound doable, Kevin?

KT: Yes ma'am.

AA: Okay.

KT: They're pretty straight, straight forward.

AA: Alright. We will review it, too, with, with the client.

JB: Thank you so much.

Thank you.

AA: And hopefully we can set up a time, um, tomorrow or Monday.

KT: I will work on this, this – I, I may have a final draft by Monday to submit to you.

AA: Okay. And then maybe next week we'll, we'll do this – it's um at this point pretty time sensitive, unfortunately.

KT: I'll, I'll put as much as I can into it and hopefully have a, a draft – I may have a draft for you tomorrow, uh, at least so I can get it to Jennifer. Um, but we, it may, it may take me a little longer.

JB: Alright, you'll also have to talk to some of the – I mean to fill in the gaps in the uh

KT: Correct. I've, I've gotta talk to HomeSource to get some more of the information.

JB: You'll have _____.

AA: um, Jennifer, next week – I mean could you do it like Tuesday, the actual search? Say around Tuesday?

JB: Yes.

AA: Okay.

KT: ___. What we've got here.

BW: I, I have a conflict between 10 and 11 on Tuesday, but outside of that I assume

KT: My only conflict on Tuesday _____. 3:00 p.m.

JB: So, I'm sorry. What time were you available on Tuesday, Kevin?

KT: I'm currently available all day except 3:00 p.m.

AA: Oh, that's great. Okay.

JB: So maybe everyone could do it at noon on Tuesday for _____.

[u/k]: I can certainly hold the time, sure.

AA: Okay, so let's maybe, yea let's hold, hold noon on Tuesday, um, and then maybe aim to do it then. Does that work for everyone, and get everything we need done ahead of that time slot.

JB: Well, if we get the, uh, we will have to give a review to that, that's all. So if we get it on Monday I can review it before Tuesday, um, but uh, later than Monday.

KT: I'll have you something by Friday, but, at least Monday I can guarantee.

AA: Okay.

JB: Yea, that would be great.

AA: Okay, so let's hold Monday at noon and, and gear up for doing the search for the _____ then.

BW: I thought you said Tuesday at noon.

AA: Tuesday. I am so sorry. Tuesday at noon. I forget I say the wrong day after all of this.

[*laughter*]

AA: Okay, so thanks – thank you everyone. We'll be in touch.

BW: I'll send you a copy of the recording once it's downloaded.

AA: That would be great.

BW: Alright, I'm going to stop the recording now. Thank you.

Thank you, bye.